

WHAT IS CLAIMED IS:

1. A communication device comprising:

an encryption information determination section for

5 selecting an encryption algorithm from among a plurality of previously provided encryption algorithms, the selected encryption algorithm being different depending on a predicted total used resource or an actual total used resource;

an encryption/decryption processing section for

10 encrypting a packet in accordance with the encryption algorithm selected by the encryption information determination section; and

a communication processing section for transmitting the packet encrypted by the encryption/decryption processing section.

15 2. The communication device according to claim 1,

wherein,

the total used resource is a total of CPU utilization

rates of applications to be executed by a CPU of the communication

device, and

20 the encryption/decryption processing section performs

code processing using the CPU.

3. The communication device according to claim 1,

further comprising a resource monitoring section for monitoring

25 a current amount of used resource,

wherein the encryption information determination section calculates the total used resource based on the amount of used resource notified from the resource monitoring section.

5 4. The communication device according to claim 3, wherein,

 the encryption information determination section includes a used amount resource information memory for storing the amount of used resource notified from the resource monitoring 10 section, and calculates the total used resource based on an average of the amount of used resource stored in the used resource amount information memory for a predetermined period.

5 5. The communication device according to claim 1, 15 wherein, instead of encryption algorithms, the communication device is adapted to at least one of: authentication algorithms for performing authentication processes; or compression algorithms for performing compression/decompression processes.

20 6. The communication device according to claim 1, wherein, from among the plurality of previously provided encryption algorithms, the encryption information determination section selects an encryption algorithm such that the predicted total used resource when using the encryption algorithm does not exceed a 25 first reference value.

7. The communication device according to claim 6,
wherein the encryption information determination section includes
an encryption process and used-resource table storing a load of
5 code processing for each encryption algorithm, and calculates a
total used resource when using the encryption algorithm based on
the encryption process and used-resource table.

8. The communication device according to claim 6,
10 wherein the encryption information determination section selects,
from among encryption algorithms such that the total used resource
when using each encryption algorithm does not exceed a
predetermined tolerable value, an encryption algorithm having a
highest encryption strength.

15

9. The communication device according to claim 6,
wherein the total used resource is a total of an amount of used
resource by an encrypted communication application and an amount
of used resource by a non-encrypted communication application,
20 the encrypted communication application being defined as an
application which requires code processing, and the non-encrypted
communication application being defined as an application which
does not require code processing.

25 10. The communication device according to claim 1,

wherein, if an average of the total used resource for a predetermined period up to a point during code processing is higher than a second reference value, the encryption information determination section selects an encryption algorithm having a lower load than the 5 currently-used encryption algorithm.

11. The communication device according to claim 1, wherein, if an average of the total used resource for a predetermined period up to a point during code processing is lower than a third reference value, the encryption information determination section 10 selects an encryption algorithm having a higher encryption strength than the currently-used encryption algorithm.

12. The communication device according to claim 1, 15 wherein the encryption information determination section reselects an encryption algorithm if a difference between an actual total used resource in a point in the past and an actual total used resource at present is equal to or greater than a predetermined value.

20

13. The communication device according to claim 1, wherein the encryption information determination section previously negotiates a plurality of encryption algorithms to be used with a communication counterpart of the communication device, 25 and when the encryption/decyption processing section encrypts a

packet, selects a different encryption algorithm depending on the predicted total used resource or the actual total used resource from among the plurality of previously negotiated encryption algorithms.

5

14. The communication device according to claim 1, further comprising a schedule section for accepting a preprogramming of an application to be executed and registering execution of the application to a schedule,

10 wherein, based on a total used resource at a point in the future as predicted according to the schedule, the encryption information determination section selects an encryption algorithm to be used at that point.

15 15. The communication device according to claim 14, wherein,

the schedule comprises a schedule and used-resource table for registering, a start time, an end time, and a used resource amount for each task involved in a preprogrammed application,

20 the schedule section accepts a preprogramming of an application to be executed and registers execution of a task involved in the application to the schedule and used-resource table, and

25 for each task involved in an encrypted communication application being defined as an application which requires code

processing, the encryption information determination section selects an encryption algorithm such that the predicted total used resource when using the encryption algorithm does not exceed a first reference value during a period in which the task is executed.

5

16. The communication device according to claim 14, wherein,

the schedule comprises a schedule and used-resource table for registering, a start time, an end time, and a used resource 10 amount for each task involved in a preprogrammed application, and an event and used-resource table for registering the total used resource for a respective event slot defined by the start time and the end time of each task,

the schedule section accepts a preprogramming of an 15 application to be executed and registers execution of a task involved in the application to the schedule and used-resource table, and generates the event and used-resource table based on the schedule and used-resource table, and

for each event slot, the encryption information 20 determination section selects an encryption algorithm such that the total used resource does not exceed a first reference value during the event slot as an encryption algorithm to be used for a task involved in an encrypted communication application defined as an application which requires code processing.

25

17. The communication device according to claim 14,
wherein the schedule section registers to the schedule a preprocess
of generating a key for encrypted communications prior to starting
tasks involved in an encrypted communication application being
5 defined as an application which requires code processing, and
determines a start time of the preprocess based on a value obtained
by subtracting from a tolerable amount of used resource a total
used resource in a period existing before a scheduled start time
of a task involved in the encrypted communication application.

10

18. The communication device according to claim 14,
wherein, when it is unacceptable to register an additional
preprogramming to the schedule because the total used resource
would exceed a tolerable amount of used resource, the schedule
15 section reselects an encryption algorithm such that an encryption
algorithm whose use is already registered to the schedule is
replaced by an encryption algorithm having a smaller load if such
is possible.

20

19. The communication device according to claim 14,
wherein, when it is unacceptable to register an additional
preprogramming to the schedule because the total used resource
would exceed a tolerable amount of used resource, the schedule
section changes a time to execute an application which is already
25 registered to the schedule or changes an average data transfer

amount for encrypted communications.

20. The communication device according to claim 14,
wherein, when a preprogramming of an application which was
5 registered to the schedule is canceled, the schedule section
reselects an encryption algorithm such that an encryption algorithm
whose use is already registered to the schedule is replaced by
an encryption algorithm having a higher encryption strength if
such is possible.

10

21. An algorithm selection method comprising:
an encryption information determination step of
selecting an encryption algorithm from among a plurality of
previously provided encryption algorithms, the selected
15 encryption algorithm being different depending on a predicted total
used resource or an actual total used resource;
a code processing step of encrypting a packet in
accordance with the encryption algorithm selected by the encryption
information determination step; and
20 a communication processing step of transmitting the
packet encrypted by the code processing step.

22. An algorithm selection program for causing a computer
to execute the steps described in claim 30.

25

23. A computer readable recording medium having recorded thereon the algorithm selection program according to claim 22.

24. A communication device comprising:

5 an encryption information determination section for
selecting an encryption algorithm from among a plurality of
previously provided encryption algorithms, the selected
encryption algorithm being different depending on an encryption
algorithm or encryption algorithms used for one or more packets
10 received from a communication counterpart;

an encryption/decryption processing section for encrypting a packet to be transmitted to the communication counterpart in accordance with the encryption algorithm selected by the encryption information determination section; and

15 a communication processing section for transmitting the
packet encrypted by the encryption/decryption processing section.

25. The communication device according to claim 24,
wherein the encryption information determination section includes
20 an encryption algorithm statistics table for storing the encryption
algorithm or encryption algorithms used for the one or more packets
received from the communication counterpart, and selects an
encryption algorithm appearing with a highest frequency among the
encryption algorithm or encryption algorithms used for the received
25 one or more packets by referring to the encryption algorithm

statistics table.

26. The communication device according to claim 24,
wherein the encryption information determination section includes
5 an encryption algorithm statistics table for storing the encryption
algorithm or encryption algorithms used for the one or more packets
received from the communication counterpart, and an encryption
process and used-resource table for storing information concerning
an encryption strength and a calculation amount of each of the
10 previously provided encryption algorithms, and selects an
encryption algorithm having a highest encryption strength among
those encryption algorithms whose calculation amounts are equal
to or less than a statistical value derived from the calculation
amounts of the encryption algorithms used for the received packets,
15 by referring to the encryption algorithm statistics table and the
encryption process and used-resource table.

27. The communication device according to claim 24,
wherein, if a packet to work as a determination material based
20 on which to select an encryption algorithm has not been received
from the communication counterpart, the encryption information
determination section causes the communication processing section
to transmit a packet which induces a response from the communication
counterpart.

28. An algorithm selection method comprising:

an encryption information determination step of selecting an encryption algorithm from among a plurality of previously provided encryption algorithms, the selected encryption algorithm being different depending on an encryption algorithm or encryption algorithms used for one or more packets received from a communication counterpart;

5 a code processing step of encrypting a packet to be transmitted to the communication counterpart in accordance with the encryption algorithm selected by the encryption information determination step; and

10 a communication processing step of transmitting the packet encrypted by the code processing step.

15 29. An algorithm selection program for causing a computer to execute the steps described in claim 44.

30. A computer readable recording medium having recorded thereon the algorithm selection program according to claim 29.

20

31. A communication system comprising a first communication device and a second communication device being coupled to the first communication device to be capable of communicating therewith, wherein the first communication device 25 is the communication device according to claim 1, and the second

communication device is the communication device according to
claim 24.

32. A communication device comprising:

5 an encryption information determination section having
a function of selecting an encryption algorithm from among a
plurality of previously provided encryption algorithms such that
the selected encryption algorithm is different depending on a
predicted total used resource or an actual total used resource,
10 and a function of selecting an encryption algorithm from among
a plurality of previously provided encryption algorithms such that
selected encryption algorithm is different depending on an
encryption algorithm or encryption algorithms used for one or more
packets received from a communication counterpart;
15 an encryption/decyption processing section for
encrypting a packet to be transmitted to the communication
counterpart in accordance with the encryption algorithm selected
by the encryption information determination section; and
 a communication processing section for transmitting the
20 packet encrypted by the encryption/decyption processing section.

33. The communication device according to claim 32,
wherein the encryption information determination section performs
a primary-subordinate negotiation process through communications
25 with the communication counterpart to confirm whether to work as

a primary or a subordinate with respect to the communication counterpart, and based on a result of the primary-subordinate negotiation process, switches between the function of selecting a different encryption algorithm depending on the predicted total used resource or the actual total used resource and the function of selecting a different encryption algorithm depending on the encryption algorithm or encryption algorithms used for the one or more packets received from the communication counterpart.

10 34. The communication device according to claim 33, wherein, in the primary-subordinate negotiation process, the encryption information determination section compares a performance of the communication device and a performance of the communication counterpart, and selects a different encryption

15 algorithm depending on the predicted total used resource or the actual total used resource if the performance of the communication device is lower than the performance of the communication counterpart, and selects a different encryption algorithm depending on the encryption algorithm or encryption algorithms used for the one or more packets received from the communication counterpart.

20 25 35. The communication device according to claim 32, wherein, instead of encryption algorithms, the communication

device is adapted to at least one of: authentication algorithms for performing authentication processes; or compression algorithms for performing compression/decompression processes.